



Web Images Groups<sup>New!</sup> News Froogle more »  
"Linear transformation" "symmetric-key ciphers"  Advanced Search Preferences

**Web** Results 1 - 2 of about 3 for "Linear transformation" "symmetric-key ciphers" daterange:2449718-245

Tip: Try removing quotes from your search to get more results.

[PDF] [This is a Chapter from the Handbook of Applied Cryptography, by A. ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... 1.13.1). The most prominent classes of attack for **symmetric-key ciphers** are (for a fixed key): 1. ciphertext-only – no additional information is available. ...

[www.cacr.math.uwaterloo.ca/hac/about/chap7.pdf](http://www.cacr.math.uwaterloo.ca/hac/about/chap7.pdf) - [Similar pages](#)

[PS] [This is a Chapter from the Handbook of Applied Cryptography, by A. ...](#)

File Format: Adobe PostScript - [View as Text](#)

... \$1.13.1). The most prominent classes of attack for **symmetric-key ciphers** are (for a ... cipher is a **linear transformation**, and falls under known-plaintext attack. ...

[www.cacr.math.uwaterloo.ca/hac/about/chap7.ps](http://www.cacr.math.uwaterloo.ca/hac/about/chap7.ps) - [Similar pages](#)

*In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.*

*If you like, you can [repeat the search with the omitted results included](#).*



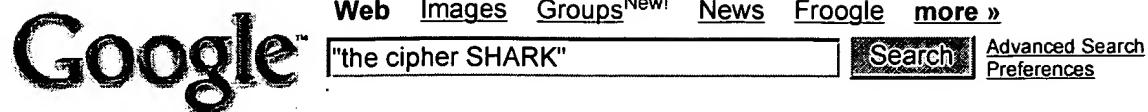
Free! [Google Desktop Search](#): Search your own computer.

"Linear transformation" "symmetric-key ciphers"

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied?](#) [Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google

**Web**Results 1 - 10 of about 190 for "**the cipher SHARK**". (0.41 seconds)**[PDF] The Cipher SHARK**File Format: PDF/Adobe Acrobat - [View as HTML](#)Page 1. 1 **The Cipher SHARK** Vincent Rijmen Joan Daemen Bart Preneel Antoon Bosselaers Erik De Win Katholieke Universiteit Leuven, ESAT ...[www.cosic.esat.kuleuven.ac.be/ publications/article-55.pdf](http://www.cosic.esat.kuleuven.ac.be/publications/article-55.pdf) - [Similar pages](#)**[PDF] The Block Cipher Square**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Page 1. 1 The Block Cipher Square Joan Daemen 1 Lars Knudsen 2 Vincent Rijmen 2 Banksys Haachtesteenweg 1442 B-1130 Brussel, Belgium ...

[www.cosic.esat.kuleuven.ac.be/ publications/article-309.pdf](http://www.cosic.esat.kuleuven.ac.be/publications/article-309.pdf) - [Similar pages](#)[ [More results from www.cosic.esat.kuleuven.ac.be](#) ]**SHARK - Wikipedia, the free encyclopedia**

... Fast Software Encryption 1997: 28–40; Vincent Rijmen, Joan Daemen, Bart

Preneel, Anton Bosselaers, Erik De Win: **The Cipher SHARK**. ...[en.wikipedia.org/wiki/Shark\\_\(cipher\)](http://en.wikipedia.org/wiki/Shark_(cipher)) - 17k - [Cached](#) - [Similar pages](#)**[PDF] The CS Block Cipher**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Page 1. The CS 2 Block Cipher Tom St Denis Secure Science Corporation tom@securescience.net Abstract. In this paper we describe our new CS 2 block cipher which ...

[eprint.iacr.org/2004/085.pdf](http://eprint.iacr.org/2004/085.pdf) - [Similar pages](#)**[PDF] Security Assessment of Hierocrypt and Rijndael against the ...**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Page 1. Security Assessment of Hierocrypt and Rijndael against the Differential and Linear Cryptanalysis (Extended Abstract) Kenji ...

[eprint.iacr.org/2001/070.pdf](http://eprint.iacr.org/2001/070.pdf) - [Similar pages](#)[ [More results from eprint.iacr.org](#) ]**[PDF] The CSQUARE Transform**File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Transforms", Cryptology ePrint Archive, Report 2004-010 [8] A. Bosselaers, J. Daemen, B. Preneel, V. Rijmen, E. De Win, "The Cipher SHARK", Fast Software ...

[libtomcrypt.org/dmwt.pdf](http://libtomcrypt.org/dmwt.pdf) - [Similar pages](#)**[PDF] Cryptographic Cryptographic Techniques Techniques Overview**File Format: PDF/Adobe Acrobat - [View as HTML](#)

... 3) V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, "The Cipher SHARK," Fast Software Encryption, LNCS 1039, pp. 99–112, 1996. ...

[www.toshiba.co.jp/rdc/security/hierocrypt/CRYPTREC/2000/out\\_3e.pdf](http://www.toshiba.co.jp/rdc/security/hierocrypt/CRYPTREC/2000/out_3e.pdf) - [Similar pages](#)**Block Cipher Components**... MDS: Ciphers using it: Shark: **The Cipher Shark** (Daemen, Rijmen, 1996); The Interpolation Attack on Block Ciphers (Thomas Jakobsen, Lars R. Knudsen, 1997). ...[www.tcs.hut.fi/~helger/crypto/link/block/components.php](http://www.tcs.hut.fi/~helger/crypto/link/block/components.php) - 6k - [Cached](#) - [Similar pages](#)**[PDF] Hardware Performance Characterization of Block Cipher Structures**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Page 1. Hardware Performance Characterization of Block Cipher Structures □

Lu Xiao and Howard M. Heys Electrical and Computer Engineering ...

[www.engr.mun.ca/~howard/PAPERS/rsa2003.pdf](http://www.engr.mun.ca/~howard/PAPERS/rsa2003.pdf) - [Similar pages](#)

[PDF] [The Block Cipher: SEA2 With Provable Resistance Against DC and LC ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Page 1. THE BLOCK CIPHER SEA2 813 Received March 6, 1999; accepted August 4, 1999. Communicated by Chi Sung Laih. JOURNAL OF ...

[www.iis.sinica.edu.tw/JISE/2000/200011\\_02.pdf](http://www.iis.sinica.edu.tw/JISE/2000/200011_02.pdf) - [Similar pages](#)

Gooooooooooooogle ►

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)



Free! [Google Desktop Search](#): Search your own computer.

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google



Web Images Groups<sup>New!</sup> News Froogle more »  
"Linear transformation" "symmetric-key ciphers"  Advanced Search Preferences

**Web** Results 1 - 1 of 1 for "Linear transformation" "symmetric-key ciphers" error-correction code. (0.25 s)

Tip: Try removing quotes from your search to get more results.

[Shark \(cipher\) - encyclopedia article about Shark \(cipher\). Free ...](#)

... size In modern cryptography, **symmetric key ciphers** are generally ... The **linear transformation** is derived from an error ... **code Reed-Solomon error correction** is a ...

[encyclopedia.thefreedictionary.com/Shark%20\(cipher\)](http://encyclopedia.thefreedictionary.com/Shark%20(cipher)) - 58k - Supplemental Result - [Cached](#) - [Similar pages](#)



Free! [Google Desktop Search](#): Search your own computer.

"Linear transformation" "symmetric-key ciphers"

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google